REMARKS

The Examiner has rejected Claims 1, 2, 4-14, 16-26 and 28-43 under 35 U.S.C. 103(a) as being unpatentable over Vairavan (U.S. Publication No. 2002/0083344 A1), in view of Drake (U.S. Patent No. 6,006,328). Applicant respectfully disagrees with such rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that it would have been obvious to combine Vairavan with Drake "because certain operating system[s] [are] more vulnerable to attacks" and "if it were an untrusted network, you would not want an outsider to penetrate your operating system." To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Vairavan and Drake references, especially in view of the vast evidence to the contrary.

One of the first inquiries in an obviousness analysis is whether all of the references relied on are analogous art. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." *In re Oetiker*, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992).

Applicant respectfully asserts that the Examiner has relied on non-analogous art to make a prior art showing of applicant's claimed invention. Applicant respectfully asserts that Vairavan teaches an invention which "overcomes the deficiencies and limitations of the prior art by providing an inter/intra-networking device that... comprises a plurality of access device cards, a packet processor, a security processor, a system processor and a switching fabric" (Paragraphs [0017]-[0022] - emphasis added). On the other hand, Drake teaches computer code protecting software against eavesdropping, local and remote tampering, examination, tracing, and spoofing by rogues (see abstract and Col. 3, lines 32-38). Clearly, combining Vairavan's inter/intra-networking device with Drake's computer code for preventing eavesdropping, local and remote tampering, examination, tracing, and spoofing by rogues, is in no way obvious as suggested by the Examiner, because the two inventions are clearly *non-analogous*. In view of the vastly different types of problems that inter/intra-networking devices address as opposed to preventing software against eavesdropping, etc., the Examiner's proposed combination is clearly inappropriate.

More importantly, with respect to the third element of the *prima facie* case of obviousness, applicant respectfully asserts that the combination of the Vairavan and Drake references fails to meet all of applicant's claim limitations. For example, with respect to independent Claims 1, 13, and 25, the Examiner has relied on Col. 4 line 47-Col. 5, line 34 and Col. 14 ,lines 33-39 from the Drake reference to make a prior art showing of applicant's claimed "conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network" (see this or similar, but not necessarily identical language in the aforementioned independent claims).

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches "several security-enhancing techniques to combat eavesdropping," including "hampering [the] examination of software-code operating system code or...parts thereof through the use of the encryption or partial encryption of said code" and "preventing the

disassembly of said code through the inclusion of dummy instructions and prefixes and additional code to mislead and hamper disassembly" (emphasis added). Additionally, the excerpt teaches "replacing software which is vulnerable to eavesdropping with equivalent software which is far more secure" (emphasis added). Applicant further notes that the only suggestion of an operating system in Drake relates to the fact that the invention in Drake "has general application to many different operating systems" under which the invention "is designed to operate."

Applicant respectfully asserts that simply disclosing including dummy instructions and prefixes to mislead and hamper disassembly of code, in addition to replacing software which is vulnerable to eavesdropping with equivalent software that is more secure, fails to suggest any sort of impersonation of an operating system, as applicant claims. Specifically, the only suggestion of an operating system in Drake relates to allowing the invention of Drake (i.e. software-based computer security enhancing process) to operate on many different operating systems, which clearly does not teach any sort of impersonating a different operating system, let alone "conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network" (emphasis added), as claimed by applicant.

Furthermore, with respect to the independent claims, the Examiner has relied on Col. 4, line 47 – Col. 5, line 34, and Col. 14, lines 33-39 from Drake to make a prior art showing of applicant's claimed "replacing the portion of outgoing network data with data characteristic of the different operating system to prevent identification of the operating system by impersonating the different operating system, for misleading attackers into attempting attacks that are unworkable on the operating system" (see this or similar, but not necessarily identical language in the independent claims).

Once again, applicant respectfully asserts that the excerpts relied on by the Examiner merely teach "several security-enhancing techniques to combat eavesdropping," including "preventing the disassembly of said code through the inclusion

of dummy instructions and prefixes and additional code to mislead and hamper disassembly (ie. obfuscating inserts)" (Col. 4, lines 47-54 - emphasis added). In addition, applicant notes that the only replacing taught by Drake relates to "replacing software which is vulnerable to eavesdropping with equivalent software which is far more secure" (Col. 5, lines 21-23). Additionally, the only disclosure of an operating system in such excerpts from Drake simply teaches that "the invention has general application to many different operating systems" (Col. 14, lines 35-36 – emphasis added).

However, the mere disclosure of "the inclusion of dummy instructions and prefixes and additional code to mislead and hamper disassembly" (emphasis added), in no way suggests "replacing the portion of outgoing network data with data characteristic of the different operating system to prevent identification of the operating system by impersonating the different operating system, for misleading attackers into attempting attacks that are unworkable on the operating system" (emphasis added), as claimed by applicant. In addition, merely replacing vulnerable software with secure software does not even suggest any sort of outgoing network data, let alone "replacing the portion of outgoing network data with data characteristic of the different operating system," in the context claimed by applicant (emphasis added). Furthermore, disclosing that the invention has general application to many operating systems, as in Drake, fails to rise to the level of specificity nor even suggest "impersonating the different operating system, for misleading attackers into attempting attacks that are unworkable on the operating system" (emphasis added), in the manner as claimed by applicant.

Additionally, with respect to independent Claim 34, the Examiner has relied on Col. 4, line 47 – Col. 5, line 34 from Drake (reproduced above) to make a prior art showing of applicant's claimed "data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system."

Again, applicant respectfully asserts that the excerpt relied on by the Examiner merely discloses "the inclusion of dummy instructions and prefixes and additional code

to mislead and hamper disassembly" (emphasis added). However, Drake's disclosure of including dummy instructions and prefixes, and additional code in no way suggests any sort of "data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system" (emphasis added), as claimed by applicant.

Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 4 et al., the Examiner has relied on the following excerpt from Vairavan to make a prior art showing of applicant's claimed technique "wherein the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data."

> "Various modules operating within the packet processor 210 and other components within the inter/intra-networking device 110 access the security policy database 315 in order to perform security and intrusion detection functions. For example, a firewall module 310 containing multiple firewalls may access the security policy database 315 to retrieve a particular security standard or packet analysis algorithm." (Paragraph [0085] - emphasis added)

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "a firewall module... may access the security policy database... to retrieve a particular security standard or packet analysis algorithm" (emphasis added). However, simply accessing a security policy database in order to perform security and intrusion detection functions, as in Vairavan, in no way suggests a technique "wherein the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data" (emphasis added), as claimed by applicant.

In addition, with respect to Claim 5 et al., the Examiner has relied on Col. 4, line 47 – Col. 5, line 34 from Drake to make a prior art showing of applicant's claimed technique "wherein the security policy further specifies replacement data for the portion of outgoing network data, the replacement data characteristic of the different operating system."

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches "several security-enhancing techniques to combat eavesdropping" including "hampering [the] examination of software-code operating system code or...parts thereof through the use of the encryption or partial encryption of said code... [and] preventing the disassembly of said code through the inclusion of dummy instructions and prefixes and additional code to mislead and hamper disassembly (ie: obfuscating inserts)" (emphasis added). Additionally, the excerpt teaches "replacing software which is vulnerable to eavesdropping with equivalent software which is far more secure" (emphasis added).

However, using dummy instructions and prefixes to mislead and hamper the disassembly of code in no way suggests "replacement data characteristic of the different operating system" (emphasis added), as claimed by applicant. Further, replacing software vulnerable to eavesdropping with more secure equivalent software fails to suggest a technique "wherein the security policy further specifies replacement data for the portion of outgoing network data, the replacement data characteristic of the different operating system" (emphasis added), as claimed by applicant.

Still yet, with respect to Claim 10 et al., the Examiner has relied on Col. 8 lines 24-63 from Drake to make a prior art showing of applicant's claimed "sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network."

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches "a method of providing for a secure entry of ID-Data in a computer system

comprising activating a visual display or animation and/or audio feedback... as part of said secure entry of ID-Data so as to hamper emulation of said secure entry process" (Col. 8, lines 25-30 - emphasis added). However, providing a secure entry of ID-Data by activating a visual display to hamper emulation fails to even suggest "sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network" (emphasis added), as claimed by applicant. Clearly, a method for a secure entry of ID-Data fails to even suggest "sending a false response" (emphasis added), in the manner as claimed by applicant.

Since at least the first and third elements of the *prima facie* case of obvious have not been met, as noted above, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P350/01.022.01).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100